*72 Geo. Wash. L. Rev. 1139, **

The George Washington Law Review

August, 2004

72 Geo. Wash. L. Rev. 1139

LENGTH: 1329 words

THE FUTURE OF INTERNET SURVEILLANCE LAW: A SYMPOSIUM TO DISCUSS INTERNET SURVEILLANCE, PRIVACY & THE USA PATRIOT ACT: FOREWORD: The Future of Internet Surveillance Law

NAME: Orin S. **Kerr***

BIO: * Associate Professor, The George Washington University Law School.

SUMMARY:
... One week after the attacks of September 11, 2001, the Bush administration introduced antiterrorism legislation that offered to revamp the Internet surveillance statutes in several significant ways. ... In October 2001, Congress enacted a modified version of the administration's proposal in the form of the USA Patriot Act. ... Internet surveillance law has had a hard time grabbing scholarly attention in this environment. Judicial interpretations of the Fourth Amendment have so far allowed Internet surveillance law to develop as a primarily statutory field. ... The Law Review invited leading scholars and practitioners in the field of Internet surveillance law to Washington, D.C., on October 23, 2003, and asked them to address an important aspect of the Internet surveillance statutes. ... Within these broad guidelines, contributors were free to focus on whatever aspect of the statutory Internet surveillance laws that they wished. The goal was to advance the scholarship within the field of Internet surveillance law by presenting descriptive and normative scholarship that recognizes the statutory nature of the field. ... One contribution focuses on how the laws are implemented in practice, and another offers a comparative international perspective. ... Taken individually, each essay in this issue tackles a difficult and important issue. Viewed collectively, the essays span and even help define the field of Internet surveillance law. ...

TEXT:
[*1139]

One week after the attacks of September 11, 2001, the Bush administration introduced antiterrorism legislation that offered to revamp the Internet surveillance statutes in several significant ways. [1] Newspapers and magazines were filled with discussions of proposed amendments to a set of esoteric laws including the **Stored Communications Act,** [3] the Electronic Communications Privacy Act, [5] In October 2001, Congress enacted a modified version of the administration's proposal in the form of the USA Patriot Act. [6] Since that time, the Patriot Act and Internet surveillance law have remained hot button topics in the press. With several key surveillance provisions of the Patriot Act set to expire by 2006, [7] the public controversy over Internet surveillance laws seems likely to continue.

Despite the importance and high profile of Internet surveillance law, the field has been virtually ignored by legal scholars. The primary culprit is the heavy focus among American legal scholars on the work of the courts, and specifically, judicial interpretations of the Constitution. To many law

professors, the Supreme Court's docket of constitutional cases provides the essential guide to important issues in contemporary American law. If a field of law is primarily statutory, or if the courts have not addressed it in any depth, most law professors are inclined to ignore it. Internet surveillance law has had a hard time grabbing scholarly attention in this environment. Judicial interpretations of the Fourth Amendment have so far allowed Internet surveillance law to develop as a primarily statutory field. Further, the absence of a statutory suppression remedy for most violations of the Internet surveillance laws has resulted in few legal challenges to surveillance practices and few judicial decisions on the books. [8] Without judicial opinions to study, law professors mostly have declined to wade into the statutory morass to try to explain and critique the field.

[*1140] The absence of expert guidance has had an unfortunate effect on the public and scholarly debate about Internet surveillance law and practice. Reporters often find themselves unable to locate experts who understand the latest developments, leading to poor media coverage. Interested citizens have few sources of legal scholarship that can explain the law and its purposes. And in Washington, D.C., congressional staffers can surf Westlaw and Lexis all day but find little to explain the law or provide thoughtful perspectives from which to evaluate legislative proposals. The situation is no better for law professors, practitioners, and law students with more academic interests. Even the briefest research into the statutory surveillance laws quickly exhausts existing resources.

This issue of The George Washington Law Review is designed to address the gap in existing scholarship. The Law Review invited leading scholars and practitioners in the field of Internet surveillance law to Washington, D.C., on October 23, 2003, and asked them to address an important aspect of the Internet surveillance statutes. Participants were asked to focus their efforts in two ways. First, participants were invited to explain the existing statutory law in their area of interest. Second, participants were asked to articulate concrete proposals for legislative change that Congress could use as a point of departure in future debates. Within these broad guidelines, contributors were free to focus on whatever aspect of the statutory Internet surveillance laws that they wished. The goal was to advance the scholarship within the field of Internet surveillance law by presenting descriptive and normative scholarship that recognizes the statutory nature of the field.

The resulting symposium issue has exceeded my expectations and the expectations of the editors at the Law Review. The contributions encompass a remarkably broad range of perspectives from academics, privacy advocates, current and former prosecutors, and former legislative aides. Several of the contributions offer macroscale thematic perspectives on the field of Internet surveillance law. [9] Others offer detailed analysis of individual statutes such as the **Stored Communications Act** [11] One contribution focuses on how the laws are implemented in practice, [12] and another offers a comparative international perspective. [13] Others analyze specific recurring issues, such as the uses and misuses of commercial **[*1141]** databases [15] Finally, the former General Counsel of the Senate Judiciary Committee offers a remarkable first-hand recollection of the passage of the Patriot Act. [16]

Taken individually, each essay in this issue tackles a difficult and important issue. Viewed collectively, the essays span and even help define the field of Internet surveillance law. The contributions offer rich and thoughtful analysis of many important issues that have never been addressed in the pages of law reviews. I am confident that they will serve as a valuable resource for scholars, legislators, and the public alike.

Legal Topics:

For related research and practice materials, see the following legal topics:

Computer & Internet Law > Criminal Offenses > Search & Seizure

Computer & Internet Law > Privacy & Security > Electronic Communications Privacy Act

Criminal Law & Procedure > Sentencing > Departures

FOOTNOTES:

n1. See Chris Adams et al., Bush Seeks To Expand Legal Arsenal Against Terrorism, Wall St. J.,

Sept. 18, 2001, at A24.

n2. 18 U.S.C. 2701-2711 (2000).

n3. 18 U.S.C. 3121-3127 (2000).

n4. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

n5. Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. 1801-1811 (2000).

n6. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272.

n7. Id. 224.

n8. See generally Orin S. **Kerr,** Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law, 54 Hastings L.J. 805 (2003).

n9. Patricia L. Bellia, Surveillance Law Through Cyberlaw's Lens, 72 Geo. Wash. L. Rev. 1375 (2004); Deirdre K. Mulligan, Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act, 72 Geo. Wash. L. Rev. 1557 (2004); Daniel J. Solove, Reconstructing Electronic Surveillance Law, 72 Geo. Wash. L. Rev. 1264 (2004).

n10. Orin S. **Kerr,** A User's Guide to the **Stored Communications Act,** and a Legislator's Guide to Amending It, 72 Geo. Wash. L. Rev. 1208 (2004).

n11. Peter P. Swire, The System of Foreign Intelligence Surveillance Law, 72 Geo. Wash. L. Rev. 1306 (2004).

n12. Paul K Ohm, Parallel-Effect Statutes and E-Mail "Warrants": Reframing the Internet Surveillance Debate, 72 Geo. Wash. L. Rev. 1599 (2004).

n13. Paul M. Schwartz, Evaluating Telecommunications Surveillance in Germany: The Lessons of the Max Planck Institute's Study, 72 Geo. Wash. L. Rev. 1244 (2004).

n14. James X. Dempsey & Lara M. Flint, Commercial Data and National Security, 72 Geo. Wash. L. Rev. 1459 (2004).

n15. Clifford S. Fishman, Technology and the Internet: The Impeding Destruction of Privacy by Betrayers, Grudgers, Snoops, Spammers, Corporations, and the Media, 72 Geo. Wash. L. Rev. 1503 (2004).

n16. Beryl A. Howell, Seven Weeks: The Making of the USA PATRIOT Act, 72 Geo. Wash. L. Rev. 1145 (2004).

Source: Legal > Secondary Legal > Law Reviews & Journals > Individual Law Reviews & Journals > G - I > **George Washington Law Review**
Terms: **kerr and stored communications act** (Edit Search | Suggest Terms for My Search)
View: Full
Date/Time: Tuesday, May 6, 2008 - 11:35 AM EDT

*72 Geo. Wash. L. Rev. 1264, **

The George Washington Law Review

August, 2004

72 Geo. Wash. L. Rev. 1264

LENGTH: 27951 words

THE FUTURE OF INTERNET SURVEILLANCE LAW: A SYMPOSIUM TO DISCUSS INTERNET SURVEILLANCE, PRIVACY & THE USA PATRIOT ACT: SURVEILLANCE LAW: RESHAPING THE FRAMEWORK: Electronic Surveillance Law

NAME: Daniel J. Solove*

BIO: * Associate Professor, The George Washington University Law School; J.D. Yale Law School. Thanks to Patricia Bellia, Linda Fisher, Chris Hoofnagle, Orin **Kerr,** Raymond Ku, Peter Raven-Hansen, Stephen Saltzburg, Paul Schwartz, and Peter Swire for helpful comments on the manuscript. I would also like to thank Romana Kaleem for excellent research assistance.

SUMMARY:
... After the September 11 attacks, Congress hastily passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act"), which made several changes to electronic surveillance law. ... As James Dempsey notes, electronic surveillance captures a wide range of communications, "whether they are relevant to the investigation or not, raising concerns about compliance with the particularity requirement in the Fourth Amendment and posing the risk of general searches. ... But this is a communication consisting of video images, not the video surveillance of a communication. ... Electronic surveillance law has not kept pace with the staggering growth of technology. ... Despite the development of the Internet, e-mail, and the dizzying array of other twentieth century technologies, there have only been five major attempts at shaping electronic surveillance law - in 1934 with section 605 of the Federal Communications Act, in 1968 with Title III of the Omnibus Crime Control and Safe Streets Act, in 1978 with FISA, in 1986 with ECPA, and in 2001 with the USA PATRIOT Act. ... As technology continues to develop, the burden should be on law enforcement officials to convince Congress that a new device does not threaten individual privacy and that they should be authorized to use it with less than a warrant. ...

TEXT:
[*1264]

Introduction

After the September 11 attacks, Congress hastily passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act"), [1] which made several changes to electronic surveillance law. The Act has sparked a fierce debate. [2] The pros and cons of the USA PATRIOT Act, however, are **[*1265]** only one part of a much larger issue: How effective is the law that regulates electronic surveillance?

Today, technology has given the government an unprecedented ability to engage in surveillance. New X-ray devices can see through people's clothing, amounting to what some call a "virtual strip-search." [3] Thermal sensors can detect movement and activity via heat patterns. [4] Telephone calls can be wiretapped; places can be "bugged" with hidden recording devices; and parabolic microphones can record conversations at long distances. [5] A device known as Carnivore developed by the Federal Bureau of Investigation ("FBI") can scan through all of the e-mail traffic of an internet service provider ("ISP"). [6] Keystroke logger devices can record every keystroke typed on one's computer, [7] and these devices can be installed into a person's computer by e-mailing a computer virus called "Magic Lantern." [8] Tracking devices can relay information about a person's whereabouts. [9] One can trace cell phone calls to a person's particular location. [10]

Surveillance cameras have become ubiquitous. Britain has erected an elaborate system of video cameras which enable officials to monitor city streets through closed circuit television. [11] Called CCTV, this system has grown rapidly ever since it was first used in 1994 in response to terrorist bombings. [12] By 2001, according to estimates, Britain had one-half million surveillance cameras, one for every 120 people. [13] The United States has begun moving toward the British model. In 2002, the U.S. National Park Service **[*1266]** installed surveillance cameras around national monuments in Washington, D.C. [14]

Surveillance technology can be a useful law enforcement tool, for it provides the government with the power to watch people's activities and listen to their conversations. These profound powers, however, raise difficult problems. As with many countries throughout the world, the United States has enacted a series of laws to balance the benefits and dangers of surveillance.

Electronic surveillance law in the United States is comprised primarily of two statutory regimes: (1) the Electronic Communications Privacy Act ("ECPA"), [15] which is designed to regulate domestic surveillance; and (2) the Foreign Intelligence Surveillance Act of 1978 ("FISA"), [16] which is designed to regulate foreign intelligence gathering. While other statutes provide additional protection, ECPA and FISA are the heart of electronic surveillance law.

The USA PATRIOT Act made a number of changes in electronic surveillance law, but the most fundamental problems with the law did not begin with the USA PATRIOT Act. In this Article, I suggest that electronic surveillance law suffers from significant problems that predate the USA PATRIOT Act. The USA PATRIOT Act indeed worsened some of these problems, but surveillance law had lost its way long before. Surveillance law is thus in need of a radical reconstruction; I aim to provide some guidance to start this endeavor.

In Part I, I discuss the purpose and history of electronic law. In Part II, I analyze several problems with existing surveillance law. I begin by focusing on specific difficulties with the scope, standards, and enforcement mechanisms of the statutes. Next, I examine the more deeply rooted and systematic problems. I contend that electronic surveillance law is overly intricate and complex, that it has failed to keep pace in adapting to new technologies, and that it provides for insufficient judicial and legislative oversight. In Part III, I suggest ways in which surveillance law should be reconstructed to address these problems. Specifically, I recommend a rather radical solution: Warrants supported by probable cause should be required for most uses of electronic surveillance. I explain why this solution best resolves the existing problems with electronic surveillance law, and I argue that this approach is flexible and practical. Finally, I recommend that Congress draft a charter regulating the FBI.

I. The Purpose and History of Electronic Surveillance Law

In order to examine the effectiveness of electronic surveillance law and the methods by which to improve it, we must first articulate the goals that we **[*1267]** want the law to achieve. At a very general level, the law of electronic surveillance recognizes two things: that government surveillance is good and that it is bad. Surveillance is an important law enforcement tool, and it can be highly effective at solving and preventing crimes. Thus, we want the government to be able to engage in certain forms of surveillance. But surveillance is also a very dangerous tool, with profound implications for our freedom and democracy. Hence, we also want government surveillance to be tightly controlled.

Our electronic surveillance law was created in response to specific problems. It was thus borne out of

experience, and it is designed to redress these problems. In this Part, I discuss the animating problems and concerns of surveillance law. I examine the costs and benefits of electronic surveillance as well as the history of how and why surveillance law developed the way it did.

A. Surveillance: The Good and the Bad

Electronic surveillance is one of the central tools of modern law enforcement. It can aid significantly in the investigations of crimes, for it allows the government to watch and listen to people during their unguarded moments, when they may speak about their criminal activity. Video cameras may capture criminals in the act and aid in their identification and arrest. Surveillance can also assist in preventing crimes because it enables the government to learn about criminal activity that is afoot and to halt it before it happens. Few would argue that these are not significant benefits.

Surveillance can also prevent crime in another way. In 1791, Jeremy Bentham imagined a new architectural design for a prison which he called the Panopticon. [17] As Michel Foucault describes it:

At the periphery, an annular building; at the centre, a tower; this tower is pierced with wide windows that open onto the inner side of the ring; the peripheric building is divided into cells, each of which extends the whole width of the building ... . All that is needed, then, is to place a supervisor in a central tower and to shut up in each cell a madman, a patient, a condemned man, a worker or a schoolboy. By the effect of backlighting, one can observe from the tower, standing out precisely against the light, the small captive shadows in the cells of the periphery. They are like so many cages, so many small theatres, in which each actor is alone, perfectly individualized and constantly visible. [18]

The Panopticon achieves obedience and discipline by having all prisoners believe they could be watched at any moment. Their fear of being watched inhibits transgression. Surveillance can thus prevent crime by making people decide not to engage in it at all. More generally, surveillance is good because it is a highly effective tool for maintaining social order. We **[*1268]** want to foster a society where people are secure from theft, vandalism, assault, murder, rape, and terrorism. We thus desire social control, and surveillance can help achieve that end.

But surveillance is bad for the very same reason. George Orwell's Nineteen Eighty-Four chronicles a totalitarian government called "Big Brother" that aims for total social control. [19] Everyone is under constant fear of being watched or overheard, and everything that people do is rigidly controlled by the government. [20] In contrast to the society depicted in Orwell's novel, our society aims to be free and democratic, and our government is a far cry from Big Brother. The goal is not to suppress all individuality, to force everybody to think and act alike. Our government, however, has some of the same surveillance capabilities as Big Brother. And even when the government does not aim for total social control, surveillance can still impair freedom and democracy.

Surveillance has negative side effects that affect both the observed and the observers. For the observed, surveillance can lead to self-censorship and inhibition. [21] According to Julie Cohen: "Pervasive monitoring of every first move or false start will, at the margin, incline choices toward the bland and the mainstream." [22] Monitoring constrains the "acceptable spectrum of belief and behavior," and it results in "a subtle yet fundamental shift in the content of our character, a blunting and blurring of rough edges and sharp lines." [23] Surveillance "threatens not only to chill the expression of eccentric individuality, but also, gradually, to dampen the force of our aspirations to it." [24] Paul Schwartz argues that surveillance inhibits freedom of choice, impinging upon self-determination. [25] Surveillance rigidifies one's past; it is a means of creating a trail of information about a person. Christopher Slobogin argues that being placed under surveillance impedes one's anonymity, inhibits one's freedom to associate with others, makes one's behavior less spontaneous, and alters one's freedom of movement. [26] Surveillance's inhibitory effects are especially potent when people are engaging in political protest or dissent. People can face persecution, public sanction, and blacklisting for their unpopular political beliefs. Surveillance can make associating with disfavored groups and causes all the more difficult and precarious.

[*1269] For the observers, surveillance presents a profound array of powers that are susceptible to abuse. As Raymond Ku notes, the Framers of the Constitution were concerned about "unfettered governmental power and discretion." [27] The Framers were deeply opposed to general warrants and writs of assistance. [28] General warrants "resulted in 'ransacking' and seizure of the personal papers of political dissidents, authors, and printers of seditious libel." [29] Writs of assistance authorized "sweeping searches and seizures without any evidentiary basis." [30] As Patrick Henry declared: "They may, unless the general government be restrained by a bill of rights, or some similar restrictions, go into your cellars and rooms, and search, ransack, and measure, every thing you eat, drink, and wear. They ought to be restrained within proper bounds." [31] The problem, in short, is with the government having too much power.

Electronic surveillance presents additional problems. It is a sweeping form of investigatory power. It extends beyond a search, for it records behavior, social interaction, and everything that a person says and does. Rather than a targeted query for information, surveillance is often akin to casting a giant net, which can ensnare a significant amount of data beyond that which was originally sought. As James Dempsey notes, electronic surveillance captures a wide range of communications, "whether they are relevant to the investigation or not, raising concerns about compliance with the particularity requirement in the Fourth Amendment and posing the risk of general searches." [32] Moreover, unlike a typical search, which is often performed in a short once-and-done fashion, electronic surveillance "continues around-the-clock for days or months." [33] Additionally, in a regular search, the government comes to a suspect's house and often searches while the suspect is present; on the other hand, "the usefulness of electronic surveillance depends on lack of notice to the suspect." [34] As Justice Douglas observed, wiretapping can become "a dragnet, sweeping in all conversations within its scope."

Dissenting from Lopez v. United States, [36] where the Court upheld the use of a pocket wire recorder to record a conversation, Justice Brennan observed that surveillance "makes the police omniscient; and police omniscience **[*1270]** is one of the most effective tools of tyranny." [37] As Justice Brandeis observed:

Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded and all conversations between them upon any subject, although proper, confidential and privileged, may be overheard. Moreover, the tapping of one man's telephone line involves the tapping of the telephone of every other person whom he may call or who may call him. As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire-tapping. [38]

Furthermore, information collected by electronic surveillance can potentially be abused. Even if abuses are rare or the risk of abuse is low, the existence of legal protection is comforting and freedom-enhancing. People need a degree of control over the government in order to feel free. Freedom is not just the absence of restraints; it is a mental state, a felt reality in both structure and sentiment. Like insurance, protections against surveillance provide a sense of security.

Surveillance gives significant power to the watchers. Part of the harm is not simply in being watched, but in the lack of control that people have over the watchers. Surveillance creates the need to worry about the judgment of the watchers. Will our e-mail be misunderstood? Will our confidential information be revealed? What will be done with the information gleaned from surveillance?

Thus, the goal of surveillance law is to ameliorate these problems while at the same time allowing for effective law enforcement. This can be accomplished by providing for the oversight of government surveillance, accountability for abuses and errors, and limits against generalized forms of surveillance.

B. The Story of Surveillance Law

Electronic surveillance emerged as early as the telegraph. After the telegraph was invented in 1844, [39] technology to tap into its communications was developed shortly thereafter. Priscilla Regan notes: "During the Civil War, the Union and Confederate armies tapped each other's telegraph communications to ascertain battle plans and troop movements. Rival press organizations tapped

each other's wire communications in order to be the first to report major news items." [40]

Following the Civil War, Congress attempted to obtain telegraph messages maintained by Western Union for various investigations. [42] Editorials decried the tapping as "an outrage upon the liberties of the citizen"; [43] as a practice that "outrages every man's sense of his right to the secrets of his own correspondence"; [44] and as "hateful and repulsive to the people in general." [45] In 1880, Congress considered a bill to protect the privacy of telegrams. [46] Although the bill was abandoned, state law responded. Several courts quashed subpoenas for telegrams. [47] As the Missouri Supreme Court stated in quashing a grand jury subpoena for telegrams: "Such an inquisition, if tolerated, would destroy the usefulness of this most important and valuable mode of communication." [48] More than half of the states passed laws to prohibit the disclosure of telegraph messages by telegraph company employees. [49]

In the twentieth century, the changing nature of the type of criminal activity being prosecuted, the rise of organized police forces, and the development of more sophisticated surveillance technologies led to a profound increase in law enforcement surveillance. The rise of the mafia and large-scale crime organizations required law enforcement to find means to learn about what crimes these groups were planning. The government began to increase prosecution of certain consensual crimes, such as gambling, the use of alcohol during Prohibition, and the trafficking of drugs. Unlike robberies or assaults, which are often reported to the police, these crimes occurred through transactions in an underground market. Infiltration into this underworld (undercover work), as well as surveillance, became key tools to detect these crimes.

In earlier times, policing consisted of amateurs who merely patrolled rather than investigated. [50] But by the twentieth century, police forces transformed into organized units of professionals. [51] The FBI emerged in the early years of the twentieth century, the brainchild of Attorney General Charles Bonaparte. In 1907, Bonaparte asked Congress to authorize the creation of a detective force in the Department of Justice ("DOJ"). [52] At the time, the DOJ was borrowing investigators from the Secret Service, and Bonaparte wanted a small permanent set of investigators to work for him in the DOJ. [53] But he was rebuffed by the House Appropriations Committee. [54] Bonaparte again asked Congress in 1908, and members of Congress were very skeptical of the idea. [55] They worried about the detective force becoming a secret police,

*72 Geo. Wash. L. Rev. 1208, **

The George Washington Law Review

August, 2004

72 Geo. Wash. L. Rev. 1208

LENGTH: 20824 words

THE FUTURE OF INTERNET SURVEILLANCE LAW: A SYMPOSIUM TO DISCUSS INTERNET SURVEILLANCE, PRIVACY & THE USA PATRIOT ACT: SURVEILLANCE LAW: RESHAPING THE FRAMEWORK: A User's Guide to the **Stored Communications Act,** and a Legislator's Guide to Amending It

NAME: Orin S. **Kerr***

BIO: * Associate Professor, The George Washington University Law School.

SUMMARY:
... The privacy of stored Internet communications in the United States is governed by a federal statute known as the **Stored Communications Act** ("SCA"). ... Although a user may think of that storage space as a "virtual home," in fact that "home" is really just a block of ones and zeroes stored somewhere on somebody else's computer. ... The classifications of ECS and RCS are context sensitive: the key is the provider's role with respect to a particular copy of a particular communication, rather than the provider's status in the abstract. ... The same treatment exists for different copies of the same communication: a provider can act as an ECS with respect to one copy of a communication, as an RCS with respect to another copy, and as neither an ECS nor an RCS with respect to a third copy. ... To compel a provider of ECS to disclose contents in electronic storage for greater than 180 days or to compel a provider of RCS to disclose contents, the government has three options. ... Providers of ECS or RCS to the public ordinarily cannot disclose either content or noncontent information. ... As I have explained elsewhere, the distinction between content and noncontent information is basic to any communications network, and its functional role explains the different treatment that the two categories receive in the SCA. ...

TEXT:
[*1208]

Introduction

The privacy of stored Internet communications in the United States is governed by a federal statute known as the **Stored Communications Act** ("SCA"). [1] The SCA was enacted in 1986 as part of the Electronic Communications Privacy Act. [2] Despite its obvious importance, the statute remains poorly understood. Courts, legislators, and even legal scholars have had a very hard time making sense of the SCA. [3] The statute is dense and confusing, and few cases exist explaining how the statute works. [4] The uncertainty has made it difficult for legislators to legislate in the field, reporters to report about it, and scholars to offer scholarly guidance in this very important area of law.

This Article presents a user's guide to the SCA. My primary goal is to explain the basic structure and

text of the Act so that legislators, courts, academics, and students can understand how it works - and in some cases, how it doesn't work. I hope to explain the nuts and bolts of the statute's many distinctions and dichotomies to reveal both the statute's dynamics and its drafters' choices. I will suggest that the statute works reasonably effectively, although certainly not perfectly. The SCA is a bit outdated and has several gaps in need of legislative attention, but by and large it reflects a sound approach to the protection of stored Internet communications. I will also explore some of the present controversies that surround how best to interpret the SCA. In particular, the recent United States Court of Appeals for the Ninth Circuit decision in Theofel v. Farey-Jones, [5] offers a new view of the SCA's basic structure that is quite different from the traditional understanding **[*1209]** that the Justice Department has followed. Similarly, the United States Court of Appeals for the First Circuit is reviewing en banc a panel opinion in United States v. Councilman [6] that departs considerably from accepted understandings of the line between the SCA and the Wiretap Act. Future litigation on these issues appears inevitable, and those working with the SCA need to understand how Theofel and Councilman depart from the traditional understanding.

In the final section of the Article, I will use my explanation of the SCA as a point of departure for analyzing how Congress should amend the statute in the future. I recommend four specific ways that Congress should rework the SCA to better protect the privacy of stored Internet communications, clarify its protections, and update the statute for the present. Specifically, I argue that Congress should: (1) raise the threshold the government must satisfy to compel the contents of certain Internet communications; (2) simplify the statute dramatically by eliminating the confusing categories of "electronic communication service" and "remote computing service"; (3) repeal 18 U.S.C. 2701 because its primary effect has been to confuse the courts; and (4) restructure the remedies scheme for violations of the statute.

I. Why the **Stored Communications Act** Exists

To understand the SCA, it helps to begin by considering why Congress enacted the statute in the first place. We need to start with the Fourth Amendment and see why the architecture of the Internet raises several puzzling issues for the scope of Fourth Amendment protection. A brief excursion into how the Fourth Amendment applies to the Internet will explain the function and importance of the SCA.

The Fourth Amendment offers strong privacy protections for our homes in the physical world. [7] Absent special circumsta